

# Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

*G. Johnson*

**December 19, 2001**

**U.S. Department of Energy**

Lawrence  
Livermore  
National  
Laboratory

## DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

This report has been reproduced directly from the best available copy.

Available electronically at <http://www.doe.gov/bridge>

Available for a processing fee to U.S. Department of Energy  
and its contractors in paper from  
U.S. Department of Energy  
Office of Scientific and Technical Information  
P.O. Box 62  
Oak Ridge, TN 37831-0062  
Telephone: (865) 576-8401  
Facsimile: (865) 576-5728  
E-mail: [reports@adonis.osti.gov](mailto:reports@adonis.osti.gov)

Available for the sale to the public from  
U.S. Department of Commerce  
National Technical Information Service  
5285 Port Royal Road  
Springfield, VA 22161  
Telephone: (800) 553-6847  
Facsimile: (703) 605-6900  
E-mail: [orders@ntis.fedworld.gov](mailto:orders@ntis.fedworld.gov)  
Online ordering: <http://www.ntis.gov/ordering.htm>

OR

Lawrence Livermore National Laboratory  
Technical Information Department's Digital Library  
<http://www.llnl.gov/tid/Library.html>

# Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

Gary Johnson<sup>1</sup>

## Summary

*Many organizations worldwide develop standards that affect nuclear instrumentation and control (I&C). Two of the primary standards organizations are the US IEEE's Nuclear Power Engineering Committee (NPEC), and the IEC subcommittee on Reactor Instrumentation (SC45A). Today, nuclear power is very much an international industry. In this environment it is vital that the activities of these standards organizations be in harmony.*

*This paper surveys the contents of the two sets of standards. Opportunities to improve consistency between the two sets are identified. It is hoped that this paper will excite a discussion of what might practically be done to improve the harmony between IEEE and IEC nuclear power standards.*

## Introduction

The collections of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, IEEE standards go to great depth on environmental qualification of many specific types of components, while IEC covers the topic only at the general level. Conversely, certain IEC standards deal with specific instrumentation and control functions, a topic area where IEEE standards are largely mute. This paper studies two questions related to the above observations. Which standards in each body should be coordinated with each other? What opportunities exist for the two bodies to build on each other's standards to efficiently improve upon the coverage of their sets of standards?

Poor coordination between the two sets of standards poses a problem for the developers of systems for plant upgrades. Developers must try to address both sets of standards to avail themselves of a sufficiently broad market. Additionally, the IEEE and IEC standards together form a more comprehensive set of guidance than either set alone. If the interfaces between the standard sets were smoother, plant staff and system designers would have a better set of tools to help in the design and specification of I&C upgrades.

To understand the similarities and differences between IEC and IEEE nuclear power standards layer diagrams were developed for each set of standards.

---

<sup>1</sup> Lawrence Livermore National Laboratory, P.O. Box 808, L-632, Livermore, CA, USA 94550. Tel: +1-925-423-8834, Fax: +1-925-422-9913, e-mail: johnson27@llnl.gov

## Layer Diagrams

Layer diagrams show the structure of a set of documents from the most general to the most specific. This study used the layer structure defined by Moore for the analysis of software engineering standards [Moore, 1998]. This structure uses six layers:

- Terminology - Documents prescribing terms and vocabulary.
- Overall guidance - Documents providing guidance covering the entire collection of standards.
- Principles - Documents describing principles / objectives for use of the standards in the collection.
- Element standards - Standards that are typically the basis for compliance.
- Application guides - Documents that supplement or give advice for using standards.
- Techniques - Documents describing methods and techniques that may be helpful in accomplishing requirements or guidance of the collection of standards.

Layer diagrams were developed for both the IEEE and IEC standards. The development of layer diagrams showed that the standards from both sets of organizations may be categorized into three groups: 1) standards describing general design topics that are applicable to all, or a wide range of specific functions, 2) standards dealing with human factors engineering issues including human-machine interface design as well as human factors engineering techniques, and 3) standards dealing with specific instrumentation, control, or electrical system functions.

The combined layer diagrams developed to show the standards in each of these three categories are in Tables 1 through 4. These diagrams represent one view of the standards. Other organizations are possible, but the organization selected here is at least useful to frame the discussion below.

## Analysis

The needs for coordination may be understood by working down through the layers. The top three layers of each category are common to all diagrams. Each layer will be discussed generically. The other layers will be discussed for each category of standards. Before these are discussed there are some general comments.

The IEEE nuclear power standard set includes several general industry standards that were selected by NPEC as particularly relevant to the nuclear industry. There is no similar practice in IEC SC45A to embrace other committees' standards. The IEEE list of relevant general standards has not been updated recently. Certain software engineering and EMI standards endorsed by NRC might be added.

The IEC standards are considered industry specific standards under a general industry systems standard, IEC 61508. This is a relatively new development and the relationship between 61508 and the nuclear standards has not yet matured. No comparable relationship exists in the IEEE sphere.

The IEC depends upon IAEA safety guides to provide overall design principles for I&C systems, therefore, this analysis treats the overarching IAEA I&C safety guides as IEC principle standards. Currently these principles are provided in IAEA Safety Guides D3, "Protection System and Related Features in Nuclear Power Plants," and D8, "Safety Related Instrumentation and Control Systems in Nuclear Power Plants." These two guides are soon to be replaced by a unified guide, "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," which is draft form is designated as DS252.

# Table 1 System Standards

Terminology	IEC 60557 IEC terminology in the nuclear reactor field / IEEE 100 Standard Dictionary of Electrical and Electronic Terms			
Overall Guide	IAEA NS-R-1 Safety of Nuclear Power Plants, Design / 10 CFR 50 Domestic Licensing of Production and Utilization Facilities			
Principles	IAEA DS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants			
	IEC 61226 Instrumentation and control systems important for safety - Classification			
	IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems			
	IEEE 603 Criteria for Safety Systems			
Element Standards	Safety systems			
	Systems Requirements		Equipment Qualification	
	IEC 60671 Periodic tests and monitoring of the protection system	IEEE 338 Periodic Surveillance Testing of Safety Systems	IEC 60780 Electrical equipment of the safety system - Qualification	IEEE 323 Qualifying Class 1E Equipment
	IEC 60709 Separation within the reactor protection system	IEEE 384 Independence of Class 1E Equipment and Circuits	IEC 60772 Electrical penetration assemblies	IEEE 317 Electric Penetration Assemblies
	IEC 60639 Use of the protection system for non-safety purposes		IEEE 334 Qualifying Continuous Duty Class 1E Motors	
	IEC 60744 Safety logic assemblies		IEEE 383 Type Test of 1E Cables, Splices, & Connections	
	IEC 61497 Electrical interlocks		IEEE 535 Qualification of Class 1E Lead Storage Batteries	
	IEC 61225 Requirements for electrical supplies		IEEE 572 Qualification of Class 1E Connection Assemblies	
	PNW 45A-419 Management of Ageing	IEEE 1205 Assessing, Monitoring, and Mitigating Aging	IEEE 650 Qualification of 1E Battery Charges and Inverters	
	IEC 60987 Programmed digital computers important to safety		IEEE C37.82 Qual of Switchgear Assemblies for 1E Apps	
	IEC 62138 Software aspects for class 2 & 3 I&C	IEC 60880 Software for computers in safety systems	IEEE C37.105 Qual of 1E Protective Relays & Auxiliaries	
	IEC 60880-2 Software aspects of defence against common cause failures, use of software tools and of pre-developed software	IEEE 7-4.3.2 Digital Computers in Safety Systems		
	IEC 61500 Multiplexed data transmission		IEEE C37.98 Seismic Testing of Relays	
	IEEE 933 Definition of Reliability Programs Plans		IEEE 833 Protection of Electric Equipment from Water Hazards	
	IEEE 577 Reliability Analysis in the Design and Operation of Safety Systems			
	IEEE 336 Installation, Inspection, and Testing of I&C Equipment			
	IEEE 805 System Identification			
Application Guide	IEC 61940 A review of the application of IEC 60880	IEEE 379 Application of the Single Failure Criterion	IEC 60980 Recommended practices for seismic qualification	IEEE 344 Seismic Qualification of Class 1E Equipment
	IEC 62082 Framework for developing standards on computer based systems and software aspects	IEEE 352 Principles of Reliability Analysis for Safety Systems		
	IEC 61224 In situ response time for RTDs			
Techniques	IEC 61868 Determination and maintenance of trip setpoints			
	IEC 61971 PWR - Measurement validation for critical safety functions			
	IEC 61838 Use of probabilistic safety assessment for classification			

**Table 2 Human Factors Engineering Standards**

Terminology	IEC 60557 IEC terminology in the nuclear reactor field / IEEE 100 Standard Dictionary of Electrical and Electronic Terms		
Overall Guide	IAEA 50-C-D Safety of Nuclear Power Plants: Design / 10 CFR 50 Domestic Licensing of Production and Utilization Facilities		
	IEC 61226 Instrumentation and control systems important for safety - Classification		
Principles	IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants		
	IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems		
Element Standards	Human Factors Engineering		
	Control Rooms	Specific HMI Systems	Principles
	IEC 60964 Design of control rooms	IEC 60960 Functional design criteria for SPDS	
	IEC 61772 Main control room - visual display units (VDU)	IEC 60965 Supplementary control for remote shutdown	
Application Guide	IEC 62247 Main Control Room Design - A review of the application of IEC 60964		IEEE 1023 Application of Human Factors Engineering to Systems, Equipment, and Facilities
			IEEE 1289 Application of Human Factors Engineering in Computer Display Design
Techniques	IEC 61771 Main control-room - V&V of design		IEEE 845 Evaluation of Human System Performance
	IEC 61839 Control rooms - Functional analysis and assignment		IEEE 1082 Human Action Reliability Analysis

**Table 3 IEC Specific Function Standards**

Terminology	IEC 60557 IEC terminology in the nuclear reactor field				
Overall Guide	IAEA 50-C-D Safety of Nuclear Power Plants: Design				
	IEC 61226 Instrumentation and control systems important for safety - Classification				
Principles	IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants				
	IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems				
	Specific Functions				
	Radiation Monitoring	Core Cooling Monitoring	Neutron Monitoring	Temperature Monitoring	Other Measurements
	IEC 61504 Plant-wide radiation monitoring	IEC 60911 Monitoring core cooling - PWRs	IEC 60568 In-core neutron flux measurements	IEC 60737 In-core or primary envelope temperature	IEC 60910 Containment monitoring for early detection of events
Element Standards	IEC 60515 Radiation detectors for instrumentation and protection	IEC 61343 Monitoring core cooling - BWR	IEC 61468 Self-powered neutron detectors	PNW 45A-420 RTDs Primary Coolant Temperature Measurement in PWRs	IEC 60988 Acoustic loose parts detection
	IEC 60768 Process stream radiation monitoring for normal operating and incident conditions	IEC 62117 Monitoring core cooling during cold shutdown - PWR	IEC 61501 Wide range neutron flux monitor - Mean square voltage method		IEC 61250 Detection of leakage in coolant systems
	IEC 60951-1 Radiation monitoring accident and post-accident conditions. Part 1: General requirements Part 2: Continuously monitoring radioactive noble gases in gaseous effluents Part 3: High range area gamma radiation monitoring Part 4: Process stream Part 5: Radioactivity of air	IEC 62118 Monitoring core cooling during shutdown - RBMK			IEC 61502 Vibration monitoring of internal structures
	IEC 61031 Area gamma radiation monitoring				IEC 61505 BWR Stability monitoring

**Table 4 IEEE Specific Function Standards**

Terminology	IEEE 100 Standard Dictionary of Electrical and Electronic Terms				
Overall Guide	10 CFR 50 Domestic Licensing of Production and Utilization Facilities				
Principles	Systems Important to Safety				
	IEEE 603 Criteria for Safety Systems				
	Specific Functions				
	Electrical Systems		Cabling Systems	Radiation Monitoring	Other Functions
	IEEE 765 Preferred Power Supply		IEEE 308 Class 1E Power Systems	IEEE 628 Raceway Systems	IEEE N42.18 Continuous OnSite Radiation Monitoring
	IEEE 387 Diesel Generators		IEEE 690 Design and Installation of Cable Systems	IEEE 692 Criteria For Security Systems	
	IEEE 741 Protection of Power Systems and Equipment		IEEE N320 Emergency Rad Monitoring		
	IEEE 317 Electric Penetration Assemblies				
	Heat Tracing				
Element Standards	IEEE C37.2 Standard for Device Function Numbers and Contact Designations				
	IEEE 944 Application and Testing of Uninterruptible Power Supplies				
	IEEE 484 Design and Installation of Vented Lead Acid Batteries				
	IEEE 1290 MOV Application, Protection, Control, & Test				
	IEEE 622 Design and Installation of Heat Tracing				
Application Guide	IEEE 450 Maintenance, Testing, and Replacement of Vented Lead Acid Batteries				
	IEEE 622A Installation of Electric Pipe Heat Tracing				
	IEEE 485 Sizing Lead Acid Batteries for Stationary Applications				
	IEEE 622B Testing and Startup for Electric Heat Tracing				
	IEEE 1106 Maintenance, Testing, and Replacement of Nickel Cadmium Batteries				
	IEEE 1050 I&C Grounding				

### *Terminology*

The IEEE and IEC take different approaches to terminology standards. The IEC attempts provide one definition of each term and coordinate each definition with other international bodies such as ISO and IAEA. The IEEE does not make a concerted attempt to uniquely define terminology, but simply catalogs each definition used in its standards with the expectation that writers will not develop a new definition where an old one will do. In any case, it is obvious that terminology should be coordinated to the extent practicable, but that some degree of inconsistency can be tolerated.

### *Overall guidance*

Neither the IEEE nor IEC standards organizations provide the overall guidance for nuclear power systems. This function is reserved for national regulatory authorities. Thus the IEEE standards look to the requirements of the US Code of Federal Regulations, Section 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," and in particular to Appendix A dealing with light water reactors (LWR). IEC standards, on the other hand, must account for the regulations of all member states. It is not practical for the working groups to be familiar with such a broad range of guidance, therefore the IAEA Safety Standard NS-R-1, "Safety of Nuclear Power Plants: Design" is used as the practical source of overall guidance. NS-R-1 is approved by the member states; thus it should represent guidance that is consistent with all member states' regulations. Nevertheless, there are differences in the nature of the NRC and IAEA guidance that cause unavoidable differences in detail. For example, the NRC regulations contain very specific requirements for LWRs while the IAEA requirements cover a broad range of reactor types.

The consistency between IAEA and NRC requirements is about as good as can be expected. Further improvement would help drive improved consistency between IEC and IEEE standards, but any change will happen very slowly. Thus IEC delegates from member states that base their nuclear regulations upon 10 CFR 50 have an important responsibility to ensure IEC standards are consistent with their national regulations. IEEE on the other hand could improve applicability of their standards to the international market by having a greater awareness of IAEA requirements and guidance. This might be achieved by broader international participation in IEEE nuclear standards subcommittees and working groups. Overlapping membership between IEEE and IEC committees should be encouraged.

### *Principles*

The greatest overlap is in standards that provide basic design principles for nuclear power plant instrumentation and control systems. IAEA DS252 and IEEE 603 are comparable in purpose in that they layout fundamental strategies to assure high functional reliability of I&C systems. DS252 has a broader scope, applying to systems important to safety, not just to the safety systems which are the scope of IEEE 603. DS252 also gives guidance on the application of the principles to specific systems, general principles for human factors engineering, and general principles for I&C system lifecycle. The preparation of DS252 included a specific effort to avoid conflict between it and IEEE 603.

IEC 61226 and 61513 support the guidance of DS252. IEC 61226 provides detailed guidance on a graded approach to system integrity, which is allowed by, but not described in detail by DS252. IEC 61513 provides a more detailed discussion of the I&C system lifecycle. The preparers of DS252 also attempted to avoid conflicts with these two standards.

Coordination among these four documents is key to establishing a common foundation for the design and acceptance of nuclear power plant I&C systems. It is recommended that updates of any one of these documents strive for consistency with the other three whenever possible. Where this is not possible, an effort should be made for the three organizations to agree upon common principles toward which future updates will move.

The greater breadth of IEC standards in this area offer IEEE an opportunity to endorse or adapt international practices for graded approach and design life cycles. These areas have, to some extent, been avoided by US standards activities because these topics are at the fringe of the regulatory spotlight in the US. The advent of software-based systems, however, has made life-cycle considerations more important. New approaches such as passive safety design and risk based regulation and new issues such as diversity requirements and alternative shutdown features are increasing the regulatory attention to systems that are important to safety, but not safety. Therefore, it may be time to more formally address these topics in US standards to support the next generation of reactor designs.

#### *Element standards and application guides*

In this analysis, element standards and application guides were classified into 4 groups: 1) system requirements, 2) equipment qualification, 3) human factors engineering, 4) specific I&C functions.

##### *System requirements*

The more complicated elements of integrity strategies espoused by both IEEE 603 and IAEA DS 252 are supported by standards covering a similar set of detailed topics. It is clear here that coordination is needed between IEEE 338 and IEC 60671 (surveillance test features); IEC 60709, IEC 60639 and IEEE 384 (independence), the IEC 60880 group and IEEE 7-4.3.2 (software), and IEEE 1205 (aging management) with the IEC ageing management standard that is under development.

One of the past problems with coordination is that the current scope of IEC 60880 is very broad such that it is difficult to identify conflicts that needed to be addressed. The breadth of scope of IEC 60880 is being addressed by a new revision that is in preparation. The new revision refines the scope of the document in accordance with lessons learned from the application of the standard (IEC 69140) and from the development of a framework for standards on computer based systems (IEC 602082).

More perplexing are the areas where the coverage of the two sets of standards is different. IEC provides more guidance on specific types of safety systems such as interlocks and communications while IEEE provides more guidance on reliability analysis and assurance.

##### *Equipment qualification*

Both IEEE and IEC have high level standards addressing the fundamentals of environmental qualification. IEEE 323 and IEC 60780 cover environmental qualification. IEEE 384 and IEC 60980 cover seismic qualification. These may be the most commercially important standards of the set as they affect the marketability of a wide range of equipment. IEC recently updated IEC 60780. At that time there was a sincere effort to check the update against IEEE 323 to identify and inform the IEC working group of any conflicts. A similar effort should be conducted wherever any of these standards are updated.

IEEE has a series of standards dealing with the application of IEEE 323 to specific types of components. No parallel exists within the IEC standards set. IEC may wish to consider the need for a similar set of detailed standards.

#### *Human factors engineering*

The IEC and IEEE human factors engineering standards seem almost complementary. The IEEE standards cover design principles while the IEC standards cover specific applications of the design principles. There is a need to ensure that the guidance of these standards is consistent with each other and with the human factors engineering guidance of IAEA DS252.

#### *Standards for Specific I&C Functions*

Both IEC and IEEE produce standards that impose requirements on specific I&C functions. Remarkably, they mostly cover completely different sets of functions. The exception is radiation monitoring. In this area coordination between IEEE N42.18, IEEE N320, and the IEC 951 series of standards should be considered when any of these are updated.

In the other areas the standards are complementary. IEC covers many specific instrumentation and control functions, while IEEE has extensive standards on electrical power systems. It is not clear where the responsibility for nuclear power plant electrical power standards lay within IEC. IEC TC45 has the charter for nuclear power instrumentation, but it is not clear that it has the charter, or at the moment the proper membership, to cover electrical power systems. Other IEC committees, however, do not have the nuclear power specific background necessary and thus are not working in the area. IAEA has some guidance for electrical power systems, but this tends to be more at the principle level.

Ideally, the two groups of function standards could be used together. To do so would require resolution of any inconsistencies that may exist between these standards and the standards outlining principles for systems important to safety.

#### *Techniques*

There is very little overlap between technique standards of IEEE and IEC. In this area also the two groups of function standards could be used together.

#### **Conclusions and Recommendations**

Efforts to update existing IEEE and IEC standards should attempt to improve the harmony among the groups of standards. Groups of standards that deserve special attention towards coordination are listed in Table 5 below. Both IEEE and IEC have mechanisms for reporting issues and requisition interpretations of standards. These appear to be little used as a driver for the improvement of standards. More extensive use of these mechanisms to plan standard revisions and sharing of plans could facilitate the harmonization of the two sets of standards.

The highest priorities for harmonization are the principles group and the environmental qualification group. The principles group because harmony here will tend to drive harmonization of sub-tier standards. The environmental qualification groups because environmental and seismic qualification have a large effect on the marketability of equipment across national boundaries

**Table 5 Summary of Related Standards**

Principles	IAEA DS-252 I&C systems important to safety IEC 61226 I&C systems important for safety - classification IEC 61513 I&C for systems important to safety - General requirements for systems IEEE 603 Criteria for Safety Systems
Environmental qualification	IEC 60780 Electrical equipment of the safety system - qualification IEEE 323 qualifying class 1e equipment IEC 60980 Recommended practices for seismic qualification IEEE 344 Seismic qualification of class 1E equipment
Surveillance	IEC 60671 Periodic tests and monitoring of the protection system IEEE 338 Periodic surveillance testing of safety systems
Independence	IEC 60709 Separation within the reactor protection system IEC 60639 Use of the protection system for non-safety purposes IEEE 384 Independence of Class 1E equipment and circuits
Software	IEC 60880 Software for computers in safety systems IEC 60880-2 Software aspects of defense against CCF, use of software tools and of PDS IEC 62138 Software aspects for class 2 & 3 I&C IEEE 7-4.3.2 Digital computers in safety systems
Aging	IEEE 1205 Assessing, monitoring, and mitigating aging PNW 45A-419 Management of aging
Radiation monitoring	IEC 60951 Radiation monitoring accident and post-accident conditions IEEE N42.18 Continuous onsite radiation monitoring IEEE N320 Emergency radiation monitoring

Future work will be done to understand the detailed changes needed to improve the harmony of the above standards.

For the coordination of new standards, it is hoped that tables 1 through 4 above will provide a ready reference for working groups to learn about existing work related to their new work items.

Table 6 summarizes the relationship between IEC and IEEE standards by topic areas. Outside of the above area there is little overlap between IEEE and IEC standards. In fact, the two sets of standards might be used in a complementary manner. Ideally, conflicts between these standards and the opposite organization's principles standards should be resolved to allow their use as normative standards in both environments. Barring that, however, the IEEE standards can be considered as informative within the IEC context and vice versa.

**Table 6 IEC, IEEE, and IAEA Topic Coverage**

	IEEE/ISA	IEC	IAEA
General Integrity Requirements			
Surveillance			
Independence			
EQ - General			
EQ - Specific			
Software			
Radiation Monitoring			
Trip setpoints			
HMI			
HFE Principles			
Reliability Analysis			
Single Failure Criterion			
Electrical systems			
Security Systems			
Heat Tracing			
Interlocks			
Multiplexed Data Transmission			
Measurement validation			
Core Cooling Monitoring			
Neutron Monitoring			
Temperature Monitoring			
Containment Monitoring			
Stability Monitoring			
Leakage Monitoring			
Vibration / Loose Parts Monitoring			

#### References

Moore 1998, *Software Engineering Standards, A User's Map*, Moore, James W., IEEE Computer Society, Los Alamitos, CA, USA, 1998.